Interview Summary	Application No.	Applicant(s)	
	09/889,918	GUILLOU ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Matthew T. Henning*. (3)_____.

(2) *James Larson*. (4)_____.

Date of Interview: *04 April 2005*.

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: _____.

Identification of prior art discussed: _____.

Agreement with respect to the claims f)☐ was reached. g)☐ was not reached. h)☒ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *See Continuation Sheet*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN ONE MONTH FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

_____
Examiner's signature, if required

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)
In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: Mr. Larson called the examiner to indicate that the changes had been made but the applicants needed more time to look over the claims. The examiner said that 1 week (until April 11th 2005) would be given. Mr. Larson stated that he would call if this was insufficient amount of time after discussing it with the applicants. The examiner received a voicemail message from Mr. Larson indicating that this amount of time was not sufficient and requested that the examiner take action on the application.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	09/889,918	GUILLOU ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

All Participants:

(1) *Matthew T. Henning*.

(2) *James Larson*.

Status of Application: *Pending*

(3) _____.

(4) _____.

Date of Interview: *28 March 2005*

Time: *10:00 AM EST*

Type of Interview:
☒ Telephonic
☐ Video Conference
☐ Personal (Copy given to: ☐ Applicant ☐ Applicant's representative)

Exhibit Shown or Demonstrated: ☒ Yes ☐ No
If Yes, provide a brief description: *Claims marked to indicate the areas where the examiner found 112 errors..*

Part I.

Rejection(s) discussed:

Claims discussed:
1-18

Prior art documents discussed:

Part II.

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:
See Continuation Sheet

Part III.

☐ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.

☒ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

(Examiner/SPE Signature)

(Applicant/Applicant's Representative Signature – if appropriate)

Continuation of Substance of Interview including description of the general nature of what was discussed: Examiner indicated that the independent claims contain allowable subject matter but are not in condition for allowance due to numerous 112 errors in all the claims as well as the lack of statutory subject matter in claims 1-3. The claims were discussed in order to show Mr. Larson each type of issue with the claims (i.e. lack of antecedent basis, lack of preamble, lack of gerund phrase in method step claims, etc.) and Mr. Larson indicated that he understood the problems and would call the examiner if he had any questions. Also, the examiner pointed out that the specification needs section headings and that there should be drawings and descriptions of the drawings in the specification. The examiner suggested that the applicant make the corrections and send them in in order to further procecution. The examiner and Mr. Larson agreed that 1 week (until April 4th 2005) would be given to make the corrections and if that was not enough time Mr. Larson would call and request more time. A Copy of the fax sent to Mr. Larson of the claims with markings to indicate where corrections needed to be made is attached hereto.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Fax Cover Sheet

Date: 24 Mar 2005

To: James Larson	**From:** Matthew T Henning
Application/Control Number: 09/889,918	**Art Unit:** 2131
Fax No.: (612) 332-9081	**Phone No.:** (571) 272-3790
Voice No.: (612) 332-5300	**Return Fax No.:** (571) 273-3790
Re:	**CC:**

☐ **Urgent** ☐ **For Review** ☐ **For Comment** ☐ **For Reply** ☐ **Per Your Request**

Comments:
ATTN: James Larson Marked up copy of the claims indicating where changes need to be made. For interview scheduled for Monday March 28th, 2005. Your call will be expected at 10:00am EST.

Number of pages 47 **including this page**

CLAIMS

1. Method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1, or of the parameters derived from these values, Preamble

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \text{ and } x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

•• by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_t\}$,

•• then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**, New Line

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

•• by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

•• and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**.

2. Method according to claim 1, designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment **R** by applying the process specified in claim 1,

2

- the demonstrator sends the controller all or part of each commitment R,

• **Step 2: act of challenge d**

- the controller, after having received all or part of each commitment R, produces challenges d whose number is equal to the number of commitments R and sends the challenges d to the demonstrator,

• **Step 3: act of response D**

- the witness computes the responses D from the challenges d by applying the process specified in claim 1,

• **Step 4: act of checking**

- the demonstrator sends each response D to the controller,

case where the demonstrator has transmitted a part of each commitment R

if the demonstrator has transmitted a part of each commitment R, the controller, having the m public values $G_1, G_2, ..., G_m$, computes a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v/G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

the controller ascertains that each reconstructed commitment R' reproduces all or part of each commitment R that has been transmitted to it.

case where the demonstrator has transmitted the totality of each commitment R

if the demonstrator has transmitted the totality of each commitment R, the controller, having the m public values $G_1, G_2, ..., G_m$, ascertains that each commitment R satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v/G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

3. Method according to claim 1, designed to provide proof to an entity, known as the controller entity, of the integrity of a message M associated with an entity called a demonstrator entity, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment R by applying the process specified according to claim 1,

• **Step 2: act of challenge d**

- the demonstrator applies a hashing function h whose arguments are the message M and all or part of each commitment R to compute at least one token T,
- the demonstrator sends the token T to the controller,
- the controller, after having received a token T, produces challenges d equal in number to the number of commitments R and sends the challenges d to the demonstrator,

• **Step 3: act of response D**

- the witness computes the responses D from the challenges d by applying the process specified according to claim 1,

• **Step 4: act of checking**

- the demonstrator sends each response D to the controller,
- the controller, having the m public values G_1, G_2, ..., G_m, computes a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

- then the controller applies the hashing function h whose arguments are the message M and all or part of each reconstructed commitment R' to reconstruct the token T',
- then the controller ascertains that the token T' is identical to the token T transmitted.

4. Method according to claim 1, designed to produce the digital signature of a message M by an entity known as the signing entity, said signing entity comprising the witness;

Signing operation

4

said signing entity executes a signing operation in order to obtain a signed message comprising:

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

said signing entity executes the signing operation by implementing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment R by applying the process specified according to claim 1,

• **Step 2: act of challenge d**

- the signing party applies a hashing function h whose arguments are the message M and each commitment R to obtain a binary train,
- from this binary train, the signing party extracts challenges d whose number is equal to the number of commitments R,

• **Step 3: act of response D**

- the witness computes the responses D from the challenges d by applying the process specified according to claim 1.

5. Method according to claim 4, designed to prove the authenticity of the message M by checking the signed message through an entity called a controller;

Checking operation

- said controller entity having the signed message executes a checking operation by proceeding as follows:

• **case where the controller has commitments R, challenges d, responses D**

if the controller has commitments R, challenges d, responses D,

• • the controller ascertains that the commitments R, the challenges d and the responses D satisfy relationships of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or relationships of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

5

• • the controller ascertains that the message M, the challenges d and the commitments R satisfy the hashing function:

$$d = h(\text{message}, R)$$

• case where the controller has challenges d and responses D

if the controller has challenges d and responses D,

• • the controller reconstructs, on the basis of each challenge d and each response D, commitments R' satisfying relationships of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot D^v \bmod n$$

or relationships of the type:

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

• • the controller ascertains that the message M and the challenges d satisfy the hashing function:

$$d = h(\text{message}, R')$$

• case where the controller has commitments R and responses D

if the controller has commitments R and responses D,

• • the controller applies the hashing function and reconstructs d'

$$d' = h(\text{message}, R)$$

• • the controller device ascertains that the commitments R, the challenges d' and the responses D satisfy relationships of the type

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \ldots G_m^{d'm} \cdot D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \ldots G_m^{d'm} \cdot \bmod n$$

6. A system designed to prove, to a controller server,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of: Preamble

- m pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1, or parameters derived from these values,
- a public modulus n constituted by the product of said f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2,

said modulus and said values being linked by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n.$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of the base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that the following conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \text{ and } x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card,

the witness device comprises

- a memory zone containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments R of the witness device, to compute commitments R in the ring of integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value produced by the random value production means, r being

7

Claim 1e

such that $0 < r < n$,

• or by performing operations of the type:

$$R_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$, then by applying the Chinese remainder method;

said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses D of the witness device for the computation, on the basis of each challenge d, of a response D,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method.

- transmission means to transmit one or more commitments R and one or more responses D;

wherein there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R, d, D}.

8

7. (Twice Amended) A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,

said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1 | , or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \text{ and } x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

entity or device - the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

•• by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

•• then by applying the Chinese remainder method;

Entity or device

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means;

• **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R**,

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

//

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 | , or of the parameters derived from these values,

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \text{ and } x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

•• by performing operations of the type:

$$R_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_t\}$,

•• then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

•• by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

•• and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller, the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^V \bmod n$$

or a relationship of the type

$$R' \equiv D^V / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

the comparison means of the controller device compare each reconstructed commitment R' with all or part of each commitment R received,

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have transmitted the totality of each commitment R, the computation means and the comparison means of the controller device, having m public values G_1, G_2, ..., G_m, ascertain that each commitment R satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^V \bmod n$$

or a relationship of the type

$$R \equiv D^V / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

8. (Twice Amended) System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message M associated with an entity known as a demonstrator,

said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

- **Step 1: act of commitment R**

14

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v = 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^{v} \bmod n$$

where r is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_t\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**, New line

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

where as the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token T through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token T, of the challenges d in a number equal to the number of commitments R,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges d to the demonstrator through the connection means;

• **Step 3: act of response D**

the means of reception of the challenges d of the witness device receive each challenge d coming from the demonstrator device through the interconnection means,

the means of computation of the responses D of the witness device compute the responses D from the challenges d by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v = 1 \cdot \bmod n \text{ or } G_i = Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

•• by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

•• then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response D, New line

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

•• by performing operations of the type:

$$D_i \equiv r_1 \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

•• and then by applying the Chinese remainder method;

said method being such that there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R, d, D},

- **Step 4: act of checking**

the transmission means of the demonstrator transmit each response D to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having m public values G_1, G_2, ..., G_m, to firstly compute a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

then, secondly, compute a token T' by applying the hashing function h having as arguments the message M and all or part of each reconstructed commitment R',

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token T' with the received token T.

9. (Twice Amended) System according to claim 6, designed to produce the digital signature of a message M, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a

nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \ , \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the

public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response D,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R, d, D},

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment R to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function h whose arguments are the message M and all or part of each commitment R to compute a binary train and extract, from this binary train, challenges d whose number is equal to the number of commitments R,

• **Step 3: act of response D**

the means for the reception of the challenges d of the witness device receive each challenge d coming from the signing device through the interconnection means,

the means for computing the responses D of the witness device compute the responses D from the challenges d by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} = Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R = r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

•• by performing operations of the type:

$$R_i = r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

•• then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response D,

• either by performing operations of the type:

$$D = r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

•• by performing operations of the type:

$$D_i = r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

•• and then by applying the Chinese remainder method;

said method being such that there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R, d, D},

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses D to the signing device through the interconnection means.

10. System according to claim 9, designed to prove the authenticity of the message M by checking the signed message by means of an entity called the controller;

Checking operation

the system being such that it comprises a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device;

the signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means, in such a way that the controller device has a signed message comprising:

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

the controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

• **case where the controller device has commitments R, challenges d, responses D** if the controller has commitments R, challenges d, responses D,

• • the computation and comparison means of the controller device ascertain that the commitments R, the challenges d and the responses D satisfy relationships of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

• • the computation and comparison means of the controller device ascertain that the message M, the challenges d and the commitments R satisfy the hashing function:

$$d = h(\text{message}, R)$$

• case where the controller device has challenges d and responses D

if the controller device has challenges d and responses D,

• • the computation means of the controller, on the basis of each challenge d and each response D, compute commitments R' satisfying relationships of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot D^v \bmod n$$

or relationships of the type:

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

• • the computation and comparison means of the controller device ascertain that the message M and the challenges d satisfy the hashing function:

$$d = h(\text{message}, R')$$

• case where the controller device has commitments R and responses D

if the controller device has commitments R and responses D,

• • the computation means of the controller device apply the hashing function and compute d' such that

$$d' = h(\text{message}, R)$$

• • the computation and comparison means of the controller device ascertain that the commitments R, the challenges d' and the responses D satisfy relationships of the type

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \ldots G_m^{d'm} \cdot D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \ldots G_m^{d'm} \cdot \bmod n$$

11. A terminal device associated with an entity, taking the form especially of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card, designed to prove to a controller server:

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity;

by means of :

- m pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1, or parameters derived from these values,

- a public modulus n constituted by the product of said f prime factors $p_1, p_2, \ldots p_f$ (f being greater than or equal to 2),

said modulus and said values being related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n .$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1.

said public value G_i being the square g_i^2 of the base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \text{ and } x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n.

said terminal device comprises a witness device comprising,

- a memory zone containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v.

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments R of the witness device, to compute commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

Claim 11

$$R \equiv r^v \bmod n$$

where r is a random value produced by the random value production means, r being such that $0 < r < n$,

• or by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_t\}$ produced by the random value production means, then by applying the Chinese remainder method;

said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses D of the witness device, for the computation, on the basis of each challenge d, of a response D,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method,

• transmission means to transmit one or more commitments R and one or more responses D;

wherein there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R, d, D}.

27

12. (Twice Amended) A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments R of the witness device compute each commitment R by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v = 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response D,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

•• by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

•• and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

where as the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means;

• **Steps 2 and 3: act of challenge d, act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of **f** prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^{v} \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the fm components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response D,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

13. (Twice Amended) Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \text{ and } x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_t\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**;

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Steps 2 and 3: act of challenge d, act of response D**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**, the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T**, through the connection means, to the controller device,

said controller, after having received the token **T**, produces challenges **d** equal in number to the number of commitments **R**,

the means of reception of the challenges d of the witness device receive each challenge d coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses D of the witness device compute the responses D from the challenges d by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \text{ and } x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv$

$Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

•• by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_r\}$,

•• then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response D,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

•• by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

•• and then by applying the Chinese remainder method;

said method being such that there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R, d, D},

• **Step 4: act of checking**

the transmission means of the demonstrator send each response D to the controller device which performs the check.

14. (Twice Amended) Terminal device according to claim 11, designed to produce the digital signature of a message M, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments R of the witness device compute each commitment R by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each

challenge **d**, computes a response **D**,

- either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

- or

- - by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

- - and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means,

- **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

- **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of **f** prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ or } G_i \equiv Q_i^v \mathbf{mod}\ n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \mathbf{mod}\ n \text{ and } x^2 \equiv -g_i \mathbf{mod}\ n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \mathbf{mod}\ n$$

where r is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \mathbf{mod}\ p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

•• by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

•• and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device, through the interconnection means.

15. Controller device especially taking the form of a terminal or remote server associated with a controller entity, designed to check:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity

by means of:

- **m** pairs of public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1,
- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2, unknown to the controller device and to the associated controller entity,

said modulus and said values being related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \text{ . mod n or } G_i \equiv Q_i^{-v} \text{ mod n .}$$

where Q_i designates a private value, unknown to the controller device, associated with the public value G_i.

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that the following conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \text{ mod n} \quad \text{and} \quad x^2 \equiv -g_i \text{ mod n}$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \text{ mod n}$$

can be resolved in x in the ring of the integers modulo n.

16. Controller device according to claim 15, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller;

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity;

sid controller device being used to execute the following steps:

• **Steps 1 and 2: act of commitment R, act of challenge d**

said controller device also has means for the reception of all or part of the commitments R coming from the demonstrator device through the connection means, the controller device has challenge production means for the production, after receiving all or part of each commitment R, of the challenges d in a number equal to the number of commitments R, each challenge d comprising m integers d_j hereinafter called elementary challenges.

the controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges d to the demonstrator through the connection means;

• **Steps 3 and 4: act of response D, act of checking**

said controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the reception means of the demonstrator have received a part of each commitment R, the computation means of the controller device, having m public values G_1, G_2, ..., G_m, compute a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

the comparison means of the controller device compare each reconstructed commitment R' with all or part of each commitment R received.

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have received the totality of each commitment R, the computation means and the comparison means of the controller device, having m public values G_1, G_2, ..., G_m, ascertain that each commitment R satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

17. Controller device according to claim 15, designed to give proof to an entity, known as a controller, of the integrity of a message M associated with an entity known as a demonstrator,

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity,

said system enabling the execution of the following steps:

• **Steps 1 and 2: act of commitment R, act of challenge d**

said controller device also has means for the reception of tokens T coming from the demonstrator device through the connection means,

the controller device has challenge production means for the production, after having received the token T, of the challenges d in a number equal to the number of commitments R, each challenge d comprising m integers d_i, herein after called elementary challenges,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges d to the demonstrator through the connection means;

• **Steps 3 and 4: act of response D, act of checking**

the controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device, having m public values G_1, G_2, ..., G_m, to firstly compute a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type

$$R' = G_1^{d1} . G_2^{d2} . ... G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' = D^v/G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

then, secondly, compute a token T' by applying the hashing function h having as arguments the message M and all or part of each reconstructed commitment R',
the controller device also comprises:

- comparison means, hereinafter called the comparison means of the controller device, to compare the computed token T' with the received token T.

18. Controller device according to claim 15, designed to prove the authenticity of the message M by checking a signed message by means of an entity called a controller;
the signed message, sent by a signing device associated with a signing entity having a hashing function h (message, R), comprising:

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

Checking operation

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a signing device associated with the signing entity,
said controller device having received the signed message from the signed device, through the connection means,
the controller device comprises:

- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device;

• **case where the controller device has commitments R, challenges d, responses D**
if the controller has commitments **R**, challenges **d**, responses **D**,

• • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$R = G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^V \bmod n$$

or relationships of the type:

$$R = D^V/G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

• • the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function

$$d = h \text{ (message, R)}$$

• **case where the controller device has challenges d and responses D**
if the controller device has challenges **d** and responses **D**,

• • the computation means of the controller, on the basis of each challenge **d** and each response **D**, compute commitments **R'** satisfying relationships of the type

$$R' = G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^V \bmod n$$

or relationships of the type:

$$R' = D^V/G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

• • the computation and comparison means of the controller device ascertain that the message **M** and the challenges **d** satisfy the hashing function:

$$d = h \text{ (message, R')}$$

• **case where the controller device has commitments R and responses D**
if the controller device has commitments **R** and responses **D**,

• • the computation means of the controller device apply the hashing function and compute **d'** such that

$$d' = h \text{ (message, R)}$$

• • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$R = G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^V \bmod n$$

or relationships of the type:

$$R = D^V/G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

46